

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 27

MAILED

MAY 31 2005

U.S. PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS
AND INTERFERENCES

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JAMES Q. MI, VISHESH PARIKH and ALBERT Y. TENG

Appeal No. 2005-0588
Application 09/259,620

ON BRIEF

Before HAIRSTON, KRASS and JERRY SMITH, Administrative Patent Judges.

JERRY SMITH, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on the appeal under 35 U.S.C. § 134 from the examiner's rejection of claims 1, 3-6 and 8-38, which constitute all the claims remaining in the application.

The disclosed invention pertains to a method and apparatus for communicating between first and second computer systems. More particularly, the invention relates to the manner in which identifiers associated with the computer systems are exchanged between the computer systems.

Representative claim 1 is reproduced as follows:

1. A method comprising:

receiving a request from a first computer system for identification of a second computer system:

retrieving a processor number that identifies a processor of the second computer system;

encrypting the processor number with a key associated with the first computer system to produce a hash value; and

providing the hash value to the first computer system in response to the request.

The examiner relies on the following references:

Claus et al. (Claus)	5,120,939	June 09, 1992
Lee et al. (Lee)	5,774,544	June 30, 1998
Zdepski et al. (Zdepski)	5,825,884	Oct. 20, 1998
Linehan	6,327,578	Dec. 04, 2001

(filed Dec. 29, 1998)

Schneier, Bruce, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed., pgs. 53, 54, 185 and 186 (1996).

The following rejections are on appeal before us:

1. Claims 1, 3, 6, 8 and 21-24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the teachings of Claus in view of Lee.

2. Claims 4, 5 and 9 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the teachings of Claus and Lee.

3. Claims 10, 11, 13, 14, 25 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the teachings of Zdepski in view of Schneier and Lee.

4. Claim 12 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over the teachings of Schneier, Zdepski and Lee in view of Linehan.

5. Claims 15, 16, 18-20, 27, 30, 31, 34, 35 and 38 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the teachings of Claus and Schneier.

6. Claims 17, 28, 32 and 36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the teachings of Claus and Schneier in view of Lee.

7. Claims 29, 33 and 37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the teachings of Claus and Schneier in view of Linehan.

Rather than repeat the arguments of appellants or the examiner, we make reference to the briefs and the answer for the respective details thereof.

OPINION

We have carefully considered the subject matter on appeal, the rejections advanced by the examiner and the evidence of obviousness relied upon by the examiner as support for the rejections. We have, likewise, reviewed and taken into consideration, in reaching our decision, the appellants' arguments set forth in the briefs along with the examiner's rationale in support of the rejections and arguments in rebuttal set forth in the examiner's answer.

It is our view, after consideration of the record before us, that the evidence relied upon and the level of skill in the particular art would have suggested to one of ordinary skill in the art the obviousness of the invention as set forth in the claims on appeal. Accordingly, we affirm.

Appellants have nominally indicated that the claims on appeal stand or fall together in seven separate groups each headed by one of the seven independent claims [brief, page 12]. Since appellants have failed to appropriately argue the separate patentability of the dependent claims, the dependent claims will

stand or fall with the independent claim from which they respectively depend. See In re King, 801 F.2d 1324, 1325, 231 USPQ 136, 137 (Fed. Cir. 1986); In re Sernaker, 702 F.2d 989, 991, 217 USPQ 1, 3 (Fed. Cir. 1983).

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the examiner to establish a factual basis to support the legal conclusion of obviousness. See In re Fine, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In so doing, the examiner is expected to make the factual determinations set forth in Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed. Cir.), cert. denied, 488 U.S. 825 (1988); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 293, 227 USPQ 657, 664 (Fed. Cir. 1985), cert. denied, 475 U.S. 1017 (1986); ACS Hosp. Sys., Inc. v. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984).

These showings by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). If that burden is met, the burden then shifts to the applicant to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. See Id.; In re Hedges, 783 F.2d 1038, 1039, 228 USPQ 685, 686 (Fed. Cir. 1986); In re Piasecki, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984); and In re Rinehart, 531 F.2d 1048, 1052, 189 USPQ 143, 147 (CCPA 1976). Only those arguments actually made by appellants have been considered in this decision. Arguments which appellants could have made but chose not to make in the brief have not been considered and are deemed to be waived [see 37 CFR § 41.37(c)(1)(vii)(2004)].

We consider first the rejection of claims 1, 3, 6, 8 and 21-24 based on Claus and Lee. The examiner finds that Claus teaches the invention of independent claim 1 except that Claus fails to teach that the unique identifier is a microprocessor number. The examiner cites Lee as teaching this feature. The examiner finds that it would have been obvious to the artisan to use the microprocessor number as taught by Lee as the unique

identification number in Claus in order to improve control of the smart cards in Claus [answer, pages 4-5].

Appellants argue that Claus fails to teach or suggest that the identification number is related to the identity of a processor. Appellants argue that the identification number in Claus is related to the user of the smart card rather than to the processor of the smart card. Appellants assert that the examiner has provided no motivation to modify Claus in the manner proposed by the examiner. Finally, appellants argue that the examiner's proposed modification would render Claus' security system unsatisfactory for its intended purpose [brief, pages 12-14].

The examiner responds that the identification number in Claus is unique to the card such that the identification number identifies the card and not the user. The examiner also responds that the motivation to combine the teachings is the greater control gained by the manufacturer as taught by Lee. Finally, the examiner responds that the proposed modification would not render Claus unsatisfactory because the modification only replaces the identification number in Claus with the processor number [answer, pages 9-11].

Appellants respond that the PIN of Claus identifies the user and not the smart card. Appellants also respond that the examiner has still failed to show where the motivation for modifying Claus in view of Lee exists [reply brief, pages 2-3].

We will sustain the examiner's rejection of independent claim 1 and of the claims which depend therefrom for essentially the reasons argued by the examiner in the answer. First, we do not agree with appellants' argument that the identification number in Claus identifies a user rather than the smart card. Claus discloses that "[s]tored within memory box 550 of smart card 500 is the above-identified personal identification number (ID)_n that is unique to that card. Thus, each smart card in Claus carries a unique number (ID)_n that identifies that smart card. A company could have a single smart card in which all employees of the company use the same smart card, and all employees would have to use the same identification number (ID)_n. Thus, (ID)_n is simply a number that identifies the smart card in Claus. Because (ID)_n is nothing more than a number which identifies the smart card, this number could essentially be anything. As pointed out by the examiner, Lee teaches a reason why a manufacturer might want to track a processor serial number.

The examiner has explained why using this serial number as the number for $(ID)_n$ would provide the advantage taught by Lee. Since $(ID)_n$ is nothing more than a number, we agree with the examiner that this provides sufficient motivation to make the number $(ID)_n$ in Claus the serial number of the processor. We also disagree with appellants that this modification of Claus would somehow render Claus unsatisfactory for its intended purpose. As noted by the examiner, replacing the number $(ID)_n$ in Claus with the processor serial number as taught by Lee would have no effect on the security system in Claus. It simply replaces one number that is unique to the smart card with another number that is unique to the smart card. Thus, none of appellants' arguments are persuasive of error in the rejection.

With respect to independent claim 6, the examiner has determined that it is analogous to claim 1 and relied on the rejection of claim 1. Appellants respond with essentially the same arguments considered above with respect to claim 1 [brief, pages 14-15 and reply brief, pages 3-4].

We will sustain the examiner's rejection of independent claim 6 and the claims which depend therefrom for the reasons discussed above with respect to claim 1.

We now consider the rejection of claims 10, 11, 13, 14, 25 and 26 based on Zdepski and Schneier. With respect to independent claim 10, the examiner finds that Zdepski teaches the claimed invention except for taking steps to ensure that the public key is authentic or that the identifier uniquely identifies the platform. The examiner cites Schneier as teaching this feature. The examiner finds that it would have been obvious to the artisan to verify the public key used in Zdepski to avoid undesired key swipes as taught by Schneier. The examiner also finds that it would have been obvious to the artisan to replace the unique identifier number in Zdepski with the processor number as taught by Lee [answer, pages 6-7].

Appellants argue that the examiner has not pointed to any language in Schneier or Claus teaching selectively authorizing encryption based on identification of another processor-based system [brief, page 16].

The examiner responds that he has identified a section of Schneier which teaches digital certificates used for identification. The examiner notes that if identification fails, the artisan would understand that the entity claiming to own the key would not be able to get the key encrypted so that encryption would be selectively de-authorized [answer, page 12].

Appellants respond that the examiner's assumption that the database server public key of Zdepski is received from the database server 276 is improper. Appellants assert that the database public key could have been received from other sources [reply brief, pages 4-5].

We will sustain the examiner's rejection of independent claim 10 and the claims which depend therefrom for essentially the reasons argued by the examiner in the answer. Specifically, we agree with the examiner that the collective teachings of the references would have suggested to the artisan that an identifier key for a processor-based system would not be encrypted if it is determined that the key is not valid. We are not persuaded by appellants' argument regarding where the key is sent from. We agree with the examiner that a skilled artisan would have recognized that a processor-based system such as taught by Zdepski could generate its own identifier key and would not have to receive such an identifier from someplace else.

We now consider the rejection of claims 15, 16, 18-20, 27, 30, 31, 34, 35 and 38 based on Claus and Schneier. With respect to independent claim 15, the examiner finds that Claus teaches the claimed invention except that Claus does not teach that the encryption is a keyed hash. The examiner cites Schneier

as teaching this feature. The examiner finds that it would have been obvious to the artisan to use keyed hashes as taught by Schneier in the enciphering computation of Claus [answer, page 8].

Appellants argue that neither Claus nor Schneier teaches or suggests an instruction unit that indicates when the instruction unit receives an instruction that requests an identifier that identifies a microprocessor or an execution unit that is adapted to furnish an indication of a hash value to external pins of a microprocessor [brief, pages 17-18].

The examiner responds that elements 563 and 561 of Claus or the input port of the smart card would all meet the claimed instruction unit. The examiner also responds that the hash value of Claus is sent to a different entity which would inherently entail the hash traveling to external pins of a processor [answer, pages 12-13].

Appellants respond that neither Claus nor Schneier teaches or suggests an identifier that identifies a microprocessor. Appellants also respond that neither Claus nor Schneier teaches or suggests an instruction unit that is adapted to indicate when the instruction unit receives an instruction that requests the identifier. Appellants assert that this is not an inherent

feature of a microprocessor [reply brief, pages 5-6].

We will sustain the examiner's rejection of independent claim 15 and the claims which depend therefrom for essentially the reasons argued by the examiner in the answer. As noted above, the number (ID)_n in Claus identifies the smart card so that it can also be considered to identify the microprocessor of the smart card. The processors of the smart card and authentication device of Claus clearly have instruction units and execution units. Contrary to appellants' argument, we find that Claus teaches encryption of an identifier by an execution unit in response to receiving an instruction requesting the identifier.

With respect to independent claim 27, appellants argue that the examiner has failed to show where Claus or Schneier teaches or suggests a hash value that identifies information associated with a user of a second computer system or where this information is stored in a database that is maintained by a first computing system [brief, pages 18-19].

The examiner responds that Claus' authentication device or first computer system stores information which meets the claimed database. The examiner notes that the hash value gives access to this information thereby identifying it [answer, page 13].

Appellants respond that Claus fails to teach or suggest using a hash value to identify information that is stored in the authentication device [reply brief, pages 6-7].

We will sustain the examiner's rejection of independent claim 27 and of the claims which depend therefrom for essentially the reasons argued by the examiner in the answer. In addition to the examiner's observations, we note that the first computer of claim 27 could be read on the combination of the authentication device and the host computer of Claus or the computer to which the smart card has been afforded access. Thus, the information associated with the user recited in claim 27 can be read on either the Sn numbers associated with the smart card, which are also stored within the authentication device, or on the personal data associated with the user which is stored within the host computer.

With respect to independent claim 31, appellants argue that Claus fails to teach or suggest using a hash value to identify information associated with a user of a second computer system for the scenario in which this information is stored in a database that is maintained by a first computer system [brief, pages 19-20]. The examiner relies on the same arguments made with respect to claim 27 [answer, page 13].

Appeal No. 2005-0588
Application 09/259,620

We will sustain the examiner's rejection of independent claim 31 and the claims which depend therefrom for the same reasons discussed above with respect to claim 27.

With respect to independent claim 35, appellants and the examiner make the same arguments considered above with respect to claim 31.

We will sustain the examiner's rejection of independent claim 35 and the claims which depend therefrom for the same reasons discussed above with respect to claim 27.


In summary, we have sustained each of the examiner's rejections of the claims on appeal. Therefore, the decision of the examiner rejecting claims 1, 3-6 and 8-38 is affirmed.

Appeal No. 2005-0588
Application 09/259,620

No time period for taking any subsequent action in connection with this appeal may be extended under 37 CFR § 1.136(a)(1)(iv).

AFFIRMED


KENNETH W. HAIRSTON
Administrative Patent Judge


ERROL A. KRASS
Administrative Patent Judge

BOARD OF PATENT
APPEALS AND
INTERFERENCES

Gerry Smith
JERRY SMITH
Administrative Patent Judge

JS/ki

Appeal No. 2005-0588
Application 09/259,620

Timothy N. Trop
Trop, Pruner, Hu & Miles
8554 Katy Freeway
Suite 100
Houston, TX 77024